

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

PAUL BARON
238 TEAL CIRCLE
BERLIN, MD 21811

*on their own behalf and on behalf of
all others similarly situated,*

JURY TRIAL DEMANDED

Plaintiffs,
v.

SPRINT CORPORATION
6200 SPRINT PARKWAY
OVERLAND PARK, KS 66251

CASE NO. _____

Serve on: Department of Assessment and
Taxation
Corporate Charter Division
301 W. Preston Street
Room 801
Baltimore, MD 21201

Defendant

CLASS ACTION COMPLAINT

Plaintiff Paul Baron (“Plaintiff” or “Named Plaintiff”), on his own behalf and on behalf of all others similarly situated, through his attorneys, Cory L. Zajdel, Esq., Jeffrey C. Toppe, Esq., and David M. Trojanowski, Esq., and Z LAW, LLC, hereby submit this Class Action Complaint against Defendant Sprint Corporation (hereinafter “Sprint” or “Defendant”) and for support states as follows:

I. PRELIMINARY STATEMENT

1. Plaintiff, both individually and on behalf of those similarly situated persons (hereafter “Class Members”), brings this Class Action to secure redress against Sprint for its reckless and negligent violations of customer privacy rights.

2. Plaintiff and Class Members are Sprint customers.

3. This action arises out of Defendant’s collection of geolocation data and the unauthorized dissemination to third-parties of the geolocation data collected from its users’ cell phones.

4. Sprint admittedly sells customer geolocation data to third-parties, including but not limited to data aggregators, who in turn, are able to use or resell the geolocation data with little or no oversight by Sprint.

5. This is an action seeking damages for Sprint’s gross failure to safeguard highly personal and private consumer geolocation data in violation of federal law.

II. JURISDICTION

6. This Court has original federal subject-matter jurisdiction over this class action pursuant to 28 U.S.C. § 1331 as the sole cause of action pled in this case arises under federal law.

7. This Court has personal jurisdiction over the parties because Plaintiff is a citizen of Maryland and because Sprint transacts substantial business within the State of Maryland.

8. Venue in this judicial district is proper pursuant to 28 U.S.C. § 1391(a) because Sprint conducts substantial business in, and may be found in, this district, and Plaintiff and members of the proposed class had their geolocation data collected within the State of Maryland.

III. PARTIES

9. Plaintiff Baron is a natural person currently residing in Worcester County, Maryland.

10. Defendant Sprint Corporation is a Delaware corporation with its principal place of business in Overland Park, Kansas.

IV. FACTUAL ALLEGATIONS

Sprint’s Statutory Obligation to Protect Customers’ Personal Network Information Under the Federal Communications Act

11. As a common carrier, Sprint is obligated to protect the confidential personal information of its customers under the Federal Communications Act (“FCA”), 47 U.S.C. § 222.

12. FCA § 222(a) provides that “[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to . . . customers” The “confidential proprietary information” referred to in FCA § 222(a) is abbreviated herein as “CPI.”

13. FCA § 222(c) additionally provides that “[e]xcept as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.” The “customer proprietary network information” referred to in FCA § 222(c) is abbreviated herein as “CPNI.”

14. FCA § 222(h)(1) (emphasis added) defines CPNI as “(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and

that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier, except that term does not include subscriber list information.”

15. The Federal Communication Commissions (“FCC”) has promulgated rules to implement FCA § 222 “to ensure that telecommunications carriers establish effective safeguards to protect against unauthorized use or disclosure of CPNI.” *See* 47 CFR § 64.2001, *et seq.* (“CPNI Rules”); CPNI Order, 13 FCC Rcd. at 8195 ¶ 193.

16. The CPNI Rules limit disclosure and use of CPNI without customer approval to certain limited circumstances (such as cooperation with law enforcement), none of which are applicable to the facts here. CPNI Rules § 64.2005.

17. The CPNI Rules §§ 64.2009(b), (d), and (e) require carriers to implement safeguards to protect customers’ CPNI.

18. These safeguards include: (i) training personnel “as to when they are and are not authorized to use CPNI[;]” (ii) establishing “a supervisory review process regarding carrier compliance with the rules[;]” and (iii) filing annual compliance certificates with the FCC.

19. The CPNI Rules § 64.2010 further require carriers to implement measures to prevent the disclosure of CPNI to unauthorized individuals. For example, “carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI.” CPNI Rules § 64.2010(a).

20. As further alleged below, Sprint violated FCA § 222 and the CPNI Rules when it disclosed CPNI and CPI to third-parties without Plaintiff or Class Members’ authorization or permission.

**Sprint's Stated Privacy and Security Commitments
to Customers in its Privacy Policy and Code of Business Conduct**

21. In its Privacy Policy (“Privacy Policy”) and Code of Business Conduct (“COBC”), Sprint acknowledges its responsibilities to protect customers’ Personal Information under the FCA, the CPNI Rules, and other regulations.

22. A true and correct copy of the Privacy Policy in effect in March 2019 (last updated in March 2017), available at <https://www.sprint.com/en/legal/sprint-corporation-privacy-policy.html#infoshare>, is attached hereto as **Exhibit A**.

23. A true and correct copy of the COBC in effect in April 2019 available at [https://s21.q4cdn.com/487940486/files/doc_downloads/governance_documents/2018/Sprint-Code-of-Conduct-\(External\)-Effective-May-25-2018.pdf](https://s21.q4cdn.com/487940486/files/doc_downloads/governance_documents/2018/Sprint-Code-of-Conduct-(External)-Effective-May-25-2018.pdf) is attached hereto as **Exhibit B**.

24. In its Privacy Policy and COBC, Sprint makes binding promises and commitments to Plaintiff and Class Members, as its customers, that it will protect and secure the confidentiality of its customers’ information.

25. The Privacy Policy defines “Personal Information” as including “information you give us, such as name, postal address, telephone number, e-mail address, date of birth, social security number or other government identification number, demographics, activities, location information, and personal preferences.” Thus, “Personal Information” includes both CPI and CPNI under FCA § 222 and the CPNI Rules.

26. In its Privacy Policy, Sprint states the following about how it shares personal information:

We do not share information that identifies you personally with third parties other than as follows:

Affiliates. We may share personal and non-personal information with affiliated entities for approved business

purposes. The data may include credit-related, payment history and transactional information

Service Providers. We may share personal information with third parties who perform services on our behalf

Other Third Parties with Your Consent. We may share information with other third parties with your consent. For example, you may agree to our sharing your information with other third parties to hear about their products and services. Use of the information you agree to share will be subject to those third parties' separate privacy policies. This may include sharing information collected in connection with financial products or services, such as installment billing

Disclosures to Third Party Application and Service Providers. You may choose to use services and products offered by third parties through our Services or devices, such as third party applications. When you leave our network you may also use mobile roaming services provided by third parties. Your use of such services and applications may result in these third parties collecting your personal information and obtaining information from Sprint, including location information (when applicable). You may also choose to give personal information directly to third parties when using our Services. In each case, personal information you give a third party will be subject to its terms, conditions, and policies—not this policy. You should review a third party's privacy policy and terms of service before providing your information or using the service.

27. Sprint's legal obligations include complying with FCA § 222, the CPNI Rules, and other legal obligations that govern protection of confidential and private information.

28. As alleged below, Sprint flagrantly and repeatedly violated its commitments made to Plaintiff and Class Members in its Privacy Policy and COBC, as well as its legal obligations under the FCA and the CPNI Rules by willingly disclosing Plaintiff and Class Members' CPNI to unauthorized third-parties.

The First Discovery of Unauthorized Disclosure of CPNI

29. On May 8, 2018, Senator Ron Wyden sent a letter (“the Wyden Letter”) to Sprint President and CEO Marcelo Claure. The Wyden Letter (attached hereto as **Exhibit C**). In the Letter, Senator Wyden expressed, in very clear terms, great concern with Sprint’s handling of consumer information. It had come to Senator Wyden’s attention that a company called Securus Technologies, a major provider of correctional-facility telephone services, purchased real-time location information from major wireless carriers, and provided that information, via a self-service web portal, to the government “for nothing more than the legal equivalent of a pinky promise.”

30. In the Wyden Letter, Senator Wyden detailed how Securus confirmed to him that the web portal enabled surveillance of customers of “every major U.S. wireless carrier,” which, in Senator Wyden’s words, “needlessly exposes millions of Americans to potential abuse and unchecked surveillance by the government.”

31. Senator Wyden also explained how wireless carriers “are prohibited from sharing certain customer information, including location data, unless the carrier either has the customer’s consent or sharing is otherwise required by law.” He ultimately concluded that, “the fact that Securus provide[d] this service at all suggests that Sprint does not sufficiently control access to [its] customers’ private information.”

32. The process by which Securus obtained access to the customers’ information in the first place is part of the problem. It purchased real-time location information on Sprint’s customers “through a third party location aggregator that has a commercial relationship with the major wireless carriers . . .”

33. Sprint had no active oversight or direction in Securus’ use of Sprint customer location data.

34. In the Wyden Letter, Senator Wyden demanded that Sprint “undertake a comprehensive audit of each third party” with whom Sprint shared its customers’ personal information, and “terminate [its] data-sharing relationships with all third parties that have misrepresented customer consent or abused their access to sensitive customer data.”

35. On June 15, 2018, Sprint sent a reply letter to Senator Wyden (hereinafter “the First Sprint Letter”) (attached hereto as **Exhibit D**). In the First Sprint Letter, Sprint represented that it “takes its obligations to safeguard [its] customers’ privacy seriously.”

36. Sprint went on to say that it “may provide location information to vendors, application developers, and location aggregators, who in turn provide the information to the ultimate end-user.” Sprint, in the First Sprint Letter, did not specifically identify any of the location aggregators with whom it had or has a contractual relationship.

The Second Discovery of Unauthorized Disclosure of CPNI

37. Six months later, on January 8, 2019, Motherboard (a news outlet) ran an investigative article concerning major telecommunications carriers (including Sprint) selling access to geolocation data to third-parties (hereinafter “The Article”) (attached hereto as **Exhibit E**).

38. In the Article, the journalist gave a bounty hunter \$300 to locate a cell phone. The bounty hunter did just that using “real-time location data sold to bounty hunters that ultimately originated from the major [telecommunications carriers].”

39. The Article revealed that a company called MicroBilt was selling cell phone geolocation services with little oversight to a spread of different private industries, “ranging from car salesmen and property managers to bail bondsmen and bounty hunters” Additionally, this

“spying capability is also being resold to others on the black market who are not licensed by the company to use it . . . seemingly without MicroBilt’s knowledge.”

40. Motherboard’s investigation revealed that “a wide variety of companies can access cell phone location data, and . . . the information trickles down from cell phone providers to a wide array of smaller players, who don’t necessarily have the correct safeguards in place to protect that data.”

41. Motherboard found that some of the location aggregators were so sloppy that “anyone could geolocate nearly any phone in the United States at a click of a mouse.”

42. In response to a request for comment, Sprint told Motherboard that “protecting our customers’ privacy and security is a top priority, and we are transparent about that in our Privacy Policy . . . Sprint does not have a direct relationship with MicroBilt. If we determine that any of our customers do and have violated the terms of our contract, we will take appropriate action based on those findings.” Sprint would not clarify the contours of its relationship with Microbilt.

43. The telecommunications carriers are the beginning of a dizzying chain of data selling, where data goes from company to company, and ultimately ends up in the hands of literally anybody who is looking.

44. The information a person could obtain included the name and address of an individual, and the geolocation of that individual’s cell phone.

45. One of the data aggregators with whom Sprint contracted is called Zumigo. Zumigo contracted with MicroBilt. MicroBilt was engaged in the process of selling consumer data to literally anybody who would pay for it, including the name and address of an individual, and the geolocation of that individual’s cell phone. Some of the sectors that utilized MicroBilt’s services were landlords, car salesmen, and others conducting credit checks.

46. In essence, Sprint was relying on the end user of the location data not to abuse the data, or not to obtain the data under false pretenses. In practice, the end users exercised no oversight over the process whatsoever.

47. Three weeks after Motherboard published its story, on January 24, 2019, Senator Wyden, along with fourteen other United States Senators, sent a letter to the FCC and Federal Trade Commission (hereinafter “Second Wyden Letter”) (attached hereto as **Exhibit F**), urging the chairmen of the respective Commissions to “broadly investigate the sale of Americans’ location data by wireless carriers, location aggregators, and other third parties.”

48. The Commissions are currently investigating each of the major wireless carriers, including Sprint.

The Second Correspondence between Sprint and Senator Wyden

49. On February 15, 2019, Sprint sent Senator Wyden another letter (hereinafter “Second Sprint Letter”) (attached hereto as **Exhibit G**) explaining that it had shared data with two location aggregators over the past five years: LocationSmart and Zumigo. Ironically, Sprint noted that “Questions regarding LocationSmart’s and Zumigo’s sub-aggregators and customers are best directed to LocationSmart and Zumigo in light of contractual provisions in our agreements regarding aggregators’ confidential information.”

50. On March 13, 2019, Senator Wyden responded in a letter to Sprint, and the other telecommunications carriers (hereinafter “the Third Wyden Letter”) (attached hereto as **Exhibit H**) seeking additional information regarding Sprint’s “repeated sale and improper disclosure of customer location data” to third-parties. In the Third Wyden Letter, Senator Wyden said it was “now abundantly clear that [Sprint has] failed to be [a] good steward[] of [its] customers’ private location information.”

51. The Third Wyden Letter also chastised the telecommunications carriers for their failures to comply with a federal law that requires wireless carriers “to protect Customer Proprietary Network Information (CPNI), which includes location data.” Wyden also noted that wireless carriers are “required to report breaches of CPNI to federal law enforcement agencies.”

52. On March 26, 2019, the FTC issued an order to Sprint, among others, seeking information the agency will use to examine how it collects, retains, uses, and discloses information about consumers and their devices.

V. CLASS ACTION ALLEGATIONS

53. Plaintiff bring this action on behalf of a Class which consists of:

All Sprint customers located in any of the United States, including the District of Columbia, between April 30, 2015 and February 15, 2019.

Excluded from the Class are those individuals who now are or have ever been executives of the Defendant and the spouses, parents, siblings, and children of all such individuals.

54. The Class, as defined above, is identifiable. Plaintiff is a member of the Class.

55. The Class consists, at a minimum, of fifty million (50,000,000) individuals and is thus so numerous that joinder of all members is clearly impracticable.

56. There are questions of law and fact which are not only common to the Class but which predominate over any questions affecting only individual Class members.

57. The common and predominating questions include, but are not limited to:

- a) Whether Sprint violated FCA § 222 by its unauthorized disclosure of Plaintiff and Class Members’ CPNI to third-parties during the class period; and
- b) Whether Plaintiff and Class Members’ CPNI was accessible to unauthorized third parties during the class period.

58. Claims of Plaintiff are typical of the claims of the respective Class Members and are based on and arise out of similar facts constituting the wrongful conduct of Defendant.

59. Plaintiff will fairly and adequately protect the interests of the Class.

60. Plaintiff is committed to vigorously litigating this matter.

61. Further, Plaintiff has secured counsel experienced in handling consumer class actions and complex consumer litigation.

62. Neither Plaintiff, nor his counsel, have any interests which might cause them not to vigorously pursue this claim.

63. Common questions of law and fact enumerated above predominate over questions affecting only individual members of the Class.

64. A class action is the superior method for fair and efficient adjudication of the controversy.

65. The likelihood that individual members of the Class will prosecute separate actions in court is remote due to the time and expense necessary to conduct such litigation.

66. Counsel for Plaintiff and the Class are experienced in class actions and foresee little difficulty in the management of this case as a class action.

VI. CAUSE OF ACTION

COUNT ONE

(Unauthorized Disclosure of Customer Confidential Proprietary Network Information in Violation of 47 U.S.C. § 222)

67. Plaintiff incorporates by reference all of the allegations herein as if each and every allegation is set forth fully herein.

68. Sprint is a telecommunications common carrier engaged in interstate commerce by wire regulated by the FCA and subject to the requirements, *inter alia*, of §§ 206 and 222 of the FCA.

69. Under FCA § 206, “[i]n case any common carriers shall do, or cause or permit it to be done, any act, matter, or thing in this chapter prohibited or declared to be unlawful, or shall omit to do any act, matter, or thing in this chapter required to be done, such common carrier shall be liable to the person or persons injured thereby for the full amount of damages sustained in consequence of any such violation of the provisions of this chapter, together with a reasonable counsel or attorney’s fee, to be fixed by the court in every case of recovery, which attorney’s fee shall be taxed and collected as part of the costs in the case.”

70. FCA § 222(a) requires every telecommunications carrier to protect, among other things, its customers’ CPI.

71. FCA § 222(c) further requires every telecommunications carrier to protect, among other things, its customers’ CPNI.

72. The information disclosed by Sprint to third-parties, including but not limited to data aggregators, without Plaintiff or Class Members’ consent was CPI and CPNI under FCA § 222.

73. Sprint failed to protect the confidentiality of Plaintiff and Class Members’ CPI and CPNI, including their wireless telephone numbers, account information, private communications, and location, by divulging that information to third-parties, including but not limited to data aggregators.

74. Through its negligent and deliberate acts, including inexplicable failures to follow its own Privacy Policy, Sprint permitted access to Plaintiff and Class Members’ CPI and CPNI.

75. Sprint profited from the sale and unauthorized dissemination of Plaintiff and Class Members’ CPI and CPNI.

76. As a direct consequence of Sprint's violations of the FCA, Plaintiff and Class Members have been damaged, in an amount to be proven at trial.

77. As a direct consequence of Sprint's violations of the FCA, Sprint was unjustly enriched in an amount to be proven at trial.

78. Plaintiff and Class Members are also entitled to attorney's fees under the FCA.

VII. PRAAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully prays that this Court:

- A. Assume jurisdiction of this case;
- B. Enter an order certifying the Class under FED. R. CIV. P. 23(b)(3);
- C. Award damages in accordance with FCA § 206; and
- D. Award reasonable attorneys' fees in accordance with FCA § 206.

Respectfully submitted,

Z LAW, LLC

Dated: April 29, 2019

/s/ 28191

Cory L. Zajdel (Fed. Bar #28191)
Jeffrey C. Toppe (Fed. Bar #20804)
David M. Trojanowski (Fed. Bar #19808)
2345 York Road, Ste. B-13
Timonium, MD 21093
(443) 213-1977
clz@zlawmaryland.com
jct@zlawmaryland.com
dmt@zlawmaryland.com

Attorneys for Plaintiffs

DEMAND FOR JURY TRIAL

Plaintiff requests a jury trial for any and all Counts for which a trial by jury is permitted by law.

/s/ 28191
Cory L. Zajdel, Esquire